LATHAM & WATKINS LLP
Elizabeth L. Deeley (CA Bar No. 230798)
elizabeth.deeley@lw.com
505 Montgomery Street, Suite 2000
San Francisco, California 94111-6538
Telephone: +1.415.391.0600
Facsimile: +1.415.395.8095

Susan E. Engel (*pro hac vice*)
susan.engel@lw.com
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Telephone: +1.202.637.2200
Facsimile: +1.202.637.2201

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
1271 Avenue of the Americas
New York, NY 10020
Telephone: +1.212.906.1200
Facsimile: +1.212.751.4864

Attorneys for Defendant *Zynga Inc.*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

I.C., a minor, by and through his natural parent, NASIM CHAUDHRI, AMY GITRE, CAROL JOHNSON, LISA THOMAS, JOSEPH MARTINEZ IV, DANIEL PETRO, and CHRISTOPHER ROSIAK, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ZYNGA INC.,

Defendant.

Case No.: 4:20-cv-01539-YGR

DEFENDANT ZYNGA INC.'S NOTICE OF MOTION AND MOTION TO DISMISS SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

Hearing: October 26, 2021
Time: 2:00 p.m.
Location: Courtroom 1 – 4th Floor
Judge: Hon. Yvonne Gonzalez Rogers

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on October 26, 2021 at 2:00 p.m., or as soon thereafter as the matter may be heard, in the United States District Court for the Northern District of California, Courtroom 1, 4th Floor, located at 1301 Clay Street, Oakland, California 94612 Defendant Zynga Inc. ("Zynga") through its undersigned counsel, will, and hereby does, move to dismiss Plaintiffs I.C., a minor by and through his natural parent Nasim Chaudhri, Carol Johnson, Daniel Petro and Christopher Rosiak's ("Plaintiffs")[1] Second Amended Consolidated Class Action Complaint ("Amended Complaint" or "Am. Compl.") pursuant to Federal Rule of Civil Procedure ("FRCP") 12(b)(1). The Amended Complaint should be dismissed because Plaintiffs lack Article III standing to bring their claims.[2]

Zynga's Motion to Dismiss ("Motion") is based on this Notice, the supporting Memorandum of Points and Authorities ("Memorandum"), the Declaration of Jessup Ferris (Dkt. 72-12) filed in connection with Zynga's initial Motion to Dismiss (Dkt. 72), the complete files and records in this action, and any additional material and arguments as may be considered in connection with the hearing on the Motion.

ISSUE TO BE DECIDED

Whether the Court should dismiss Plaintiffs' Amended Complaint because Plaintiffs lack Article III standing to bring their claims.

DATED: September 20, 2021

LATHAM & WATKINS LLP

/s/ Elizabeth L. Deeley

Elizabeth L. Deeley (CA Bar No. 230798)
elizabeth.deeley@lw.com
505 Montgomery Street, Suite 2000
San Francisco, California 94111-6538
Telephone: +1.415.391.0600
Facsimile: +1.415.395.8095

[1] This Court granted Zynga's motion to compel arbitration with respect to the remaining named Plaintiffs. *See* Order Granting Mot. to Compel and Mot. to Dismiss ("MTD Order") (Dkt. 93); Am. Compl. ¶¶ 14, 23, 25.

[2] The Amended Complaint should also be dismissed under Rule 12(b)(6) for failure to state a claim. However, in accordance with this Court's order granting Zynga's initial motion to dismiss, Zynga addresses only Article III standing in this Motion.

Susan E. Engel (*pro hac vice*)
susan.engel@lw.com
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Telephone: +1.202.637.2200
Facsimile: +1.202.637.2201

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
1271 Avenue of the Americas
New York, NY 10020
Telephone: +1.212.906.1200
Facsimile: +1.212.751.4864

Attorneys for Defendant *Zynga Inc.*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

OTHER AUTHORITIES

CONSTITUTIONAL PROVISIONS

I. INTRODUCTION

The Court dismissed Plaintiffs' prior Complaint for lack of Article III standing. Plaintiffs' Amended Complaint suffers from the same problem. Plaintiffs' theory of harm still rests on a supposed risk of identity theft that has never materialized and on purported "privacy" injuries that are untethered to any traditionally recognized privacy harm. It is now clear that Plaintiffs cannot fix these defects. Accordingly, this case should now be dismissed without leave to amend.

First, like the prior Complaint, the Amended Complaint is still based primarily on speculation that Plaintiffs' identities may *someday* be stolen, *e.g.*, via account takeover or phishing scam. Plaintiffs never genuinely allege their identities have *actually* been stolen due to the data incident that occurred over two years ago. This is fundamentally insufficient in light of the Supreme Court's unequivocal holding in *TransUnion LLC v. Ramirez* that the "risk of future harm" cannot supply standing for damages claims. 141 S. Ct. 2190, 2210-11 (2021). Nor can Plaintiffs change the nature of their allegations by simply calling identity theft a "privacy" injury analogous to an "appropriation of name or likeness" tort, or "intrusion upon seclusion." Whatever they call their injury, Plaintiffs cannot obscure the reality that their allegations are still about a risk of future identity theft—and that no Plaintiff has actually had his or her identity stolen or incurred any actual harm. Nor can Plaintiffs convert this stated risk of future identity theft into new and independent standing grounds by alleging that they feel "stress" because of that future risk, or have taken preemptive and voluntary mitigation measures. Standing requirements would be far too easy to evade if such bootstrapping were sufficient to circumvent them.

Second, Plaintiffs' effort to invoke the common law privacy tort of "publicity given to private life" similarly fails. Plaintiffs allege no facts showing that the hacking attack on Zynga, which compromised only limited data, caused intimate details about their private lives to be made public. As *TransUnion* makes clear, a privacy injury can only serve as the basis for standing if it is closely related to a harm associated with a traditional privacy tort. But the facts alleged here do not come close to meeting the harm element of the tort of publicity given to

private life because the data at issue neither involves highly private information about Plaintiffs' private lives nor was made known to the public at large. *See* Restatement (Second) of Torts § 652D (1977).

Third, Plaintiffs have no standing for injunctive relief because they allege no facts that establish the required immediate threat of repeated injury, especially given their own allegations that they no longer play Zynga's games.

For all of these reasons, the Amended Complaint should be dismissed in its entirety, without leave to amend, for failure to establish Article III standing.

II. BACKGROUND

A. The Court Dismissed Plaintiffs' First Consolidated Class Action Complaint for Lack of Article III Standing

Plaintiffs' first consolidated Complaint ("Compl.") (Dkt. 67) alleged that, as a result of the security incident announced by Zynga in September 2019 (the "Attack"), "Zynga's customers have been exposed to credit and identity theft, '[credential] stuffing,' phishing scams, and other illegal and fraudulent conduct perpetrated by the criminal actors who have come into possession of the stolen PII." Compl. ¶ 5. Yet, the Complaint failed to identify any specific instance of harm befalling any Zynga player—let alone Plaintiffs—as a result of the Attack, instead resting on an alleged "imminent risk of identity theft and fraud." *Id.*

Zynga moved to dismiss for lack of Article III standing and for failure to state a claim. In conjunction with its motion, Zynga submitted a declaration explaining that only limited information for each Plaintiff was obtained in the Attack, specifically:

Petro	Email address, screen name
Rosiak	Email address, screen name
I.C.	Email address, screen name, Games with Friends password (hashed)
Johnson	Email address, screen name, Games with Friends password (hashed), Draw Something password (plaintext), date of birth, phone number

Declaration of Jessup Ferris ("Ferris Decl.") (Dkt. 72-12) ¶ 16.

Shortly before Zynga filed its reply in support of its motion to dismiss, the Supreme Court issued its decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), holding that

"the mere risk of future harm" cannot supply standing for damages claims. *Id.* at 2210-11. Zynga's reply subsequently emphasized that in light of *TransUnion*, Plaintiffs could no longer rely on the risk of future identity theft as a basis for standing. *See* Reply iso Mot. to Dismiss at 1-5 ("Reply iso MTD") (Dkt. 84). Plaintiffs filed a surreply in which they appeared to abandon the risk of future identity theft as an independent basis for standing for their damages claims and instead argued they had standing based on an "invasion of privacy" and various present harms stemming from the alleged risk of identity theft, including stress and mitigation costs. Surreply in Opp. to Mot. to Dismiss at 2-5 ("Surreply") (Dkt. 86-1).

On July 27, 2021, the Court heard argument on Zynga's motion to dismiss, limited to the issue of Article III standing. *See* Order re Hearing (Dkt. 88). The Court agreed with Zynga that Plaintiffs had failed to demonstrate an "imminent" risk of identity theft, "given the nature of the information" involved and the fact that Plaintiffs could not identify any concrete consequences they had suffered from the Attack even though it occurred "two years ago." *See* Mot. to Dismiss Hearing Tr. 13:2-11, 16:14-16 ("Tr.") (Dkt. 94). The Court further questioned whether the exposure of Zynga account passwords could give rise to an invasion of privacy, noting that such passwords are not comparable to passwords to a "bank account" or an account with other "sensitive information." *Id.* at 26:8-27:3. And the Court indicated that Plaintiffs Petro and Rosiak in any event could not establish standing because they had only emails and screen names affected, which "people disclose . . . all the time." *Id.* at 23:20-25. The Court thus dismissed the Complaint, while giving leave to amend in order to afford Plaintiffs a final opportunity to allege facts supporting a viable theory of standing. *See id.* at 29:9-18; Order Granting Mot. to Compel and Mot. to Dismiss at 3 ("MTD Order") (Dkt. 93).

B. Plaintiffs Filed An Amended Complaint

While the Amended Complaint ("Am. Compl.") (Dkt. 95) presents more detailed allegations with respect to the named Plaintiffs, it ultimately rests on the same essential injuries alleged in Plaintiffs' prior Complaint—specifically, allegations of risk of future identity theft through account compromise or phishing emails; "stress" from that alleged risk; and time spent mitigating the risk. *See, e.g.*, Am. Compl. ¶ 30 (Plaintiff Petro); ¶¶ 20-22 (Plaintiff Johnson);

¶¶ 105-118 (Plaintiff I.C.); ¶¶ 119-130 (Plaintiff Rosiak). Plaintiffs make perfunctory references to identity theft as a "privacy" injury, analogous to "appropriation of name or likeness" or "intrusion upon seclusion," *id.* ¶¶ 95 & n.43, 99 & n.47, but these references are unaccompanied by any factual allegations reflecting that any Plaintiff has actually experienced identity theft as a result of the Attack. Plaintiffs also characterize the fact of the Attack itself as a privacy injury, claiming that the Attack "publicized . . . highly private information such as login IDs, passwords, and phone numbers." *Id.* at ¶ 69.

III. LEGAL STANDARDS

To establish Article III standing, a plaintiff must "have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). An injury in fact must be both "concrete and particularized." *Id.* at 1548. "For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" *Id.* (citation omitted). To be "concrete," the injury "must actually exist" and be "'real,' and not 'abstract.'" *Id.* (citation omitted).

A defendant may challenge Article III standing not only based on the face of a plaintiff's allegations, *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014), but also by introducing affidavits or other evidence challenging jurisdictional facts, *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). In response to a factual attack, the opposing party "must furnish affidavits or other evidence necessary to satisfy its burden of establishing subject matter jurisdiction." *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004) (citation omitted). The court then assesses standing based on the evidence before it and does not "presume the truthfulness of the plaintiff's allegations." *Safe Air*, 373 F.3d at 1039; *Leite*, 749 F.3d at 1121-22 (explaining that on a factual attack, "the district court may resolve [ ] factual disputes itself").

IV. PLAINTIFFS' ALLEGATIONS BASED ON THE RISK OF FUTURE IDENTITY THEFT DO NOT SUPPORT STANDING IN LIGHT OF *TRANSUNION*

In *TransUnion*, the Supreme Court unequivocally held that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm." 141 S. Ct. at 2210-

11. Rather, plaintiffs may sue only if a "risk of future harm *materializes* and the individual suffers a concrete harm," in which case "the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages." *Id.* at 2211 (emphasis added); *see also, e.g.*, *Ward v. Nat'l Patient Account Services Solutions, Inc.*, 9 F.4th 357, 361 (6th Cir. 2021) (concluding that *TransUnion* abrogated holding that plaintiff could satisfy concreteness requirement where a statutory violation "created a material risk of harm" (citation omitted)).

Like their initial Complaint, Plaintiffs' Amended Complaint falls short of this standard, resting almost entirely on *risks* of *future* "identity theft." (The term appears 92 times in the document.) To the extent the Amended Complaint states that Plaintiffs actually have suffered identity theft, their own allegations belie their conclusory assertions. None of the facts they allege support any inference that any Plaintiff has *actually had their identity stolen*, through online account compromise, phishing emails, or otherwise. And Plaintiffs cannot bootstrap their way into Article III standing by claiming stress based on the hypothetical risk of future identity theft or time spent changing passwords on unrelated accounts.

A. Plaintiffs Cannot Establish Standing Based on a Risk of Identity Theft That Has Not Materialized

Plaintiffs rehash their prior allegations that their online accounts might someday be compromised; or that they might someday fall for a phishing scam. But their allegations do not support any inference that any of them has actually been the victim of identity theft. Whatever new detail the Amended Complaint adds to Plaintiffs' allegations, they still fail to demonstrate any *present* harm and thus do not suffice for standing under *TransUnion*.

Risk of online account compromise. The Amended Complaint includes various allegations about Plaintiffs' reuse of passwords, in an attempt to fortify the claim that the Attack poses a risk of unauthorized access to their other accounts. In particular, Plaintiff I.C. alleges that he used his Zynga password on "90% of his online accounts," Am. Compl. ¶ 105, and Plaintiff Johnson alleges she used the same password for her Zynga account and for her "email account which she uses to send confidential information such as financial information." *Id.*

¶ 20.[3] But these allegations, even if more particularized, still do not establish any present, concrete harm, because Plaintiffs do not allege that any of I.C.'s or Johnson's accounts were *actually* accessed by an unauthorized actor, much less that any harm came to them as a result. At most, the allegations suggest a hypothetical *risk* that an unauthorized actor *could in the future* access an account, obtain sensitive information, and use it to perpetrate fraud of some type. Such future risk, in the absence of any allegations that such risk has actually "materialize[d]," is precisely what *TransUnion* forecloses as a basis for standing. *See TransUnion*, 141 S. Ct. at 2210-11.

Plaintiff I.C. tries to substantiate his claims by alleging that *attempts* were made after the Attack to gain unauthorized access to certain of his other gaming accounts unrelated to Zynga. *See* Am. Compl. ¶¶ 106, 109, 112-13. But these allegations only prove the point—he lacks any basis to allege that the attempts *succeeded*, let alone caused him some sort of harm. In particular, I.C. alleges no facts reflecting actual unauthorized activity in the accounts at issue. *Cf., e.g.*, *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027-28 (9th Cir. 2018) (noting that certain plaintiffs alleged that hackers actually "took over their AOL accounts and sent advertisements to people in their address books"). Rather, he alleges receiving emails indicating that the sites in question had *detected* suspicious login attempts. Am. Compl. ¶¶ 106, 109, 112.[4] If anything, these allegations reflect that many online platforms have mechanisms in place to monitor for and block such attempts—providing one more reason why Plaintiffs' alleged concerns about account compromise are speculative to begin with. Moreover, while I.C. suggests that these notifications

---

[3] Rosiak includes an even weaker allegation that he "used the email address compromised in the data breach to receive banking, credit union, and credit card information and notices." Am. Compl. ¶ 123. But Rosiak does not allege that his email *account* was compromised, and—to state the obvious—obtaining a person's email address does not somehow confer access to the account itself. Indeed, Rosiak does not even allege that he ever created a Zynga password or used the same password for his Zynga account and his email; nor could he, since the Ferris Declaration confirms that Rosiak did not *have* a Zynga password affected by the Attack at all. Ferris Decl. ¶ 16.

[4] Two of the emails were emails from the sites notifying I.C. of detected suspicious login activity on his gaming accounts. *Id.* ¶¶ 106, 112. A third email contained a security code sent by a gaming site for login purposes—but I.C. alleges no facts indicating that any unauthorized actor received the code or was actually able to log in to the gaming account in question. *Id.* ¶ 109.

show that he has been targeted for "identity theft," *id.* ¶ 113, he does not identify the accounts at issue other than describing them as gaming accounts, and he makes no allegation that they were used, or even could have been used, to make fraudulent charges using his identity.

Where the Amended Complaint does make conclusory allegations that identity theft has actually occurred, they amount to non sequiturs. For example, I.C. claims "based on information and belief" that his "identity has been stolen to set up accounts with financial institutions," citing an email from a financial institution that he received. *Id.* ¶ 111. But the email on its face is a routine piece of spam (about the financial institution's "updated look") that in no way suggests I.C.'s identity has been used to set up any financial account. *Id.* Indeed, the sort of information needed to set up a financial account—such as social security numbers—is not even collected by Zynga and was not affected by the Attack, for I.C. or anyone else. *See* Ferris Decl. ¶¶ 6-10, 16. I.C. does not identify any actual financial account that was opened in his name, nor does he have any plausible basis to assert that any such event happened as a result of the Attack.

Plaintiff Rosiak makes similarly unfounded allegations. He attempts to connect the Attack to what he calls a "breach of his Facebook account," Am. Compl. ¶ 35, but what he describes does not appear to be a breach of the account, and in any event, he alleges no facts plausibly connecting it to the Attack. Rosiak merely alleges that in January 2020, a couple of weeks after receiving a notification about the Attack from a dark web-monitoring service he uses (but four months after the Attack itself), he received a separate notification from the same service that his Facebook name, phone number, and user ID had been found in a data set being traded online. Nowhere does the notification indicate that Rosiak's *Facebook account itself* had been compromised. Nor does the inclusion of this basic information in a data set imply any compromise of the account; indeed, Facebook itself has explained how databases of such information have been assembled by malicious actors in the past using *publicly accessible* Facebook features, without any sort of account compromise involved.[5] But regardless, Rosiak

[5] *See* Declaration of Serrin Turner ("Turner Decl."), Ex. A, Facebook, *The Facts on News Reports About Facebook Data*, https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/ (Apr. 6, 2021).

provides no reason to connect the notification he received about this Facebook data to the Attack. The mere fact that he received the notification a couple weeks after he was notified about the Attack (and months after the Attack itself) hardly implies they are related. And Rosiak fails to provide any causal explanation for how the Attack could have led to any breach of his Facebook account—because there is none. The only Rosiak data affected by the Attack consists of his Zynga screen name and email address, which obviously would not provide access to a Facebook account.[6] *See Antman v. Uber Techs., Inc.*, No. 15-cv-01175-LB, 2018 WL 2151231, at *10 (N.D. Cal. May 10, 2018) (holding that alleged credit card fraud was not traceable to data breach where breach did not disclose information needed to commit fraud).

Plaintiffs' attempt to shoehorn their account compromise allegations into the language of privacy does not change the analysis. In the course of making these allegations, Plaintiffs claim that "[t]he data breach has allowed identity thieves to appropriate to their own use or benefit the name and personal information of the Plaintiffs and Class Members"—invoking the privacy tort of appropriation of name or likeness. Am. Compl. ¶ 95 & n.43. In similar fashion, they allege "credential stuffing invades the privacy of the Plaintiffs and Class Members by intruding into their private matters and private accounts"—invoking the privacy tort of intrusion upon seclusion. Am. Compl. ¶ 99 & n.47. But these new labels don't eliminate the old problem: because Plaintiffs do not allege they have actually experienced identity theft, they have no basis to claim that an identity thief has "appropriated" their "name or likeness" or "intruded" upon their "seclusion." As described above, no Plaintiff alleges any *actual* unauthorized access of any

[6] Rosiak alleges that he had a Zynga password that was compromised in the Attack as well, citing the notification he received about the Attack. Am. Compl. ¶ 120. However, Zynga's records confirm that only Rosiak's email address and screen name were affected by the Attack; he did not *have* a Zynga password. Ferris Decl. ¶¶ 7, 16-17. The third-party notification is unauthenticated hearsay that does not provide "competent proof" otherwise. *Leite*, 749 F.3d at 1121; *see also, e.g.*, *Elofson v. McCollum*, No. 15-CV-05761-BLF, 2017 WL 2877099, at *2 (N.D. Cal. July 6, 2017) (explaining that evidence considered on motion to dismiss for lack of jurisdiction "must be admissible"), *aff'd sub nom. Elofson v. Bivens*, 774 F. App'x 409 (9th Cir. 2019); *Yhudai v. Mortg. Elec. Registration Sys., Inc.*, No. CV1505035MMMJPRX, 2015 WL 5826777, at *7 n.38 (C.D. Cal. Oct. 2, 2015) (same). Indeed, the notification itself only provides a series of asterisks next to the term "password," which could simply reflect a null value. Am. Compl. ¶ 120. Tellingly, Rosiak never alleges that he ever created a Zynga password. Nor does he allege that he reused any purported Zynga password on his Facebook account, so it would not provide any causal explanation for any supposed breach of that account in any event.

account of theirs, let alone one containing sensitive information about their private lives. Plaintiffs cannot rely on the "mere risk of future harm"—whether privacy-related or not—to establish standing. *TransUnion*, 141 S. Ct. at 2210-11.

Risk of phishing scam. Plaintiffs fare no better with their allegations about phishing emails. Plaintiffs I.C., Rosiak, and Johnson allege that they received various suspicious emails, which they contend were sent for "likely exploitive" purposes, such as "to tempt a person to click on a link and provide additional valuable PII." *See* Am. Compl. ¶¶ 101, 107 (I.C.); *id.* ¶ 125 (Rosiak); *id.* ¶ 21 (Johnson). But Plaintiffs do not allege that they were actually "exploited" as a result of any phishing email or that they actually clicked on any link. They merely allege that they received suspicious communications, not that any harm materialized from them. At most, the allegations point to a hypothetical risk of *future* injury from the possibility that they might one day fall for a phishing scam—which cannot confer standing under *TransUnion*.

Moreover, Plaintiffs do not allege any plausible causal connection between the suspicious communications they say they received and the Attack. They hypothesize that the data affected in the Attack *could* be used to send "targeted phishing attacks made up to look as if they are an official communication from Zynga," *id.* ¶ 101, but they do not allege receiving any such Zynga-specific phishing email (let alone falling for such an email). Rather, the suspicious communications they cite have no apparent link to the Attack on their face. *See id.* ¶ 128 (alleging that Rosiak received a phishing email purporting to be sent by Wells Fargo bank). The mere fact that Plaintiffs received the alleged communications after the Attack is of no consequence; unsolicited email communications—including phishing emails—are commonplace. Indeed, Plaintiffs acknowledge that they received such communications before the Attack as well. *See id.* ¶ 21 (alleging that Johnson has experienced an "increase" in phishing emails since the Attack).

Where Plaintiffs do attempt to tie the Attack to supposed "suspicious" communications, their reasoning makes no sense. In particular, Plaintiff Rosiak points to "friend suggestions" that he received on Facebook containing people of Middle Eastern descent, which he tries to link to

the Attack on the basis that the self-professed hacker behind the Attack claims to be Pakistani. *See id.* ¶ 126. Putting aside that Plaintiffs have absolutely no basis to link these people to the perpetrator of the Attack based merely on assumptions about their shared ethnicity, these "friend suggestions" are not phishing communications to begin with, or even *communications from other individuals* at all. As the term itself reflects, they are merely "friend suggestions"—which are suggestions *made by Facebook* of people that a user may wish to become Facebook friends with, which occasionally include people that a user may not know. *See* Turner Decl., Ex. B, Facebook Help Center, *I'm seeing people I don't know suggested as People You May Know on Facebook*, https://www.facebook.com/help/415968568455523/?helpref=related (acknowledging that the feature sometimes "recommend[s] someone who you don't know"). It is telling that Plaintiffs engage in such free association in an attempt to conjure up some basis for standing. These friend suggestions only underscore that the "suspicious communications" Plaintiffs cite have nothing to do with the Attack, let alone provide a basis to sue over it.[7]

B. Plaintiffs Cannot Manufacture Standing by Claiming "Stress" and Mitigation Efforts from the Risk of Future Identity Theft

Plaintiffs Johnson's and Rosiak's alleged "alarm, stress, and concern" about the possibility that their personal information could be misused in the future, Am. Compl. ¶¶ 22, 130, and Plaintiffs I.C.'s, Johnson's, and Rosiak's alleged time spent changing their passwords on other accounts, *id.* ¶¶ 20, 116, 124, cannot supply the basis for standing; Plaintiffs cannot bootstrap their way into Article III standing by claiming present harms based on the speculative risk of identity theft.

Stress and concern. Plaintiffs "cannot manufacture standing" by claiming stress and concern based on the speculative possibility that they might someday become victims of identity

[7] Similarly, Plaintiff Petro alleges he "began to receive Facebook friend requests from individuals with whom he had no connection," as well as "spam and robo calls on his cell phone." Am. Compl. ¶ 30. But, like Rosiak, Petro alleges no facts sufficient to support an inference that the friend requests and calls were in any way connected to the Attack, particularly given that Zynga's records confirm that Petro did not have a phone number or any Facebook information affected by the Attack. Ferris Decl. ¶¶ 16, 19. Petro does not allege otherwise. *See* Am. Compl. ¶ 30 (acknowledging that information affected was "email address and Zynga screen name").

theft. *Clapper v. Amnesty Int'l*, 568 U.S. 398, 416 (2013). Allegations of present harm based on the risk of future harm suffice, if at all, only where the future harm is "certainly impending." *Id.*; *see also TransUnion*, 141 S. Ct. at 210-11 & n.7. And here, Plaintiffs simply cannot show any certainly impending or imminent risk of identity theft.

As Zynga explained in its initial motion to dismiss, and as this Court has already recognized, the compromised information at issue in this case does not give rise to the type of risk that might arise when sensitive information like social security numbers is compromised. *See* Zynga's Initial Motion to Dismiss at 5-10 ("MTD") (Dkt. 72); Tr. 13:17-14:21 (remarking that cases finding standing in data breach context have involved "more sensitive information"); *id.* at 16:14-16 (indicating that Plaintiffs could not establish standing under the "risk-of-harm cases" "given the nature of the information"); MTD Order at 3 (holding that plaintiffs did not sufficiently allege "a risk of future harm based on the information allegedly stolen in the breach"). Moreover, Plaintiffs' alleged concerns about the possibility that their Zynga passwords could be used to compromise other accounts are negated by their own statements that they have changed the passwords on their other accounts since the Attack. Am. Compl. ¶¶ 20, 116, 124. Two years have passed since the Attack, and Plaintiffs still identify *no* actual instance of identity theft or fraud. *See* Tr. 13:2-20 (recognizing that given the passage of "two years," the period of "imminent" risk has passed). Because Plaintiffs cannot establish any "certainly impending" or "imminent" risk of future harm, Plaintiffs' allegations of "alarm, stress, and concern," Am. Compl. ¶¶ 22, 130, from that hypothetical, non-imminent risk are likewise insufficient for standing. *See Clapper*, 568 U.S. at 415-16, 422; *Payne v. Off. of the Commr. of Baseball*, 705 F. App'x. 654, 655 (9th Cir. 2017) (rejecting allegations of "general anxiety" as a basis for standing where anxiety was based on future harm that was not certainly impending); *cf. Travis v. Assured Imaging LLC*, No. CV-20-00390-TUC-JCH, 2021 WL 1862446, at *10 (D. Ariz. May 10, 2021) (rejecting allegations of "emotional distress" and "anxiety" as basis for standing in data breach case). Indeed, if Plaintiffs could establish standing merely by asserting stress about any future risk, no matter how speculative, *TransUnion*'s core holding—and the fundamental requirements of Article III standing—would be far too easy to evade. *See, e.g.*, *Shelby Advocs. for Valid*

Elections v. Hargett, 947 F.3d 977, 983 (6th Cir.) (explaining that allowing plaintiffs to "bootstrap their way into standing" based on "fears of hypothetical future harm" would "eviscerate the Article III standing imperative" (citation omitted)), *cert. denied*, 141 S. Ct. 257 (2020).

Changing passwords. Plaintiffs' allegations that they spent time changing their passwords on other accounts also fail to establish standing. *See* Am. Compl. ¶¶ 20, 116, 124. Zynga reset all passwords the Attack impacted, thereby eliminating any risk of unauthorized access to its own platform. Ferris Decl. ¶ 18. But Zynga has no control over a player's choice to use the same password on other accounts, and it is common knowledge that individuals should avoid doing so, especially on sensitive accounts. *See, e.g.*, Federal Trade Commission, *It's National Password Day* (March 15, 2018), https://www.consumer.ftc.gov/blog/2018/03/its-national-password-day ("Don't reuse passwords used on other accounts."); *see also* Tr. 28:21-23 ("[I]t certainly is not smart to use passwords for your bank accounts as the same passwords you choose for everything else."). That Plaintiffs allegedly decided only *after* the Attack to make sure they were using different passwords for different accounts—something that everyone should do anyway whether they have been affected by a data breach or not—does not turn this proper practice into an "injury," let alone one traceable to *Zynga*. *See, e.g.*, *Petro-Chem Processing, Inc. v. E.P.A.*, 866 F.2d 433, 438 (D.C. Cir. 1989) (explaining that where a plaintiff's alleged injury was "due to the [plaintiff's] own fault," it was not fairly traceable to the challenged conduct); *cf. In re Equifax, Inc., Customer Data Sec. Breach Litig.*, No. 1:17-MD-2800-TWT, 2019 WL 926999, at *5 (N.D. Ga. Jan. 28, 2019) (declining to find standing where plaintiffs' alleged mitigation costs consisted of "nothing more than the exercise of ordinary due diligence in monitoring their creditworthiness"). Moreover, changing a password takes only a few moments—"too trifling" an inconvenience to "support constitutional standing." *Skaff v. Meridien N. Am. Beverly Hills, LLC*, 506 F.3d 832, 839-40 (9th Cir. 2007) (rejecting standing theory based on one-hour delay in making available a wheelchair-accessible hotel shower); *see also* Tr. 14:24-15:7 (recognizing that changing a password takes "30 seconds"); *Hernandez v.*

Path, Inc., No. 12-cv-01515 YGR, 2012 WL 5194120, at *2 (N.D. Cal. 2012) (finding de minimis harm insufficient for standing).

V. PLAINTIFFS HAVE NOT ALLEGED A "PRIVACY" INJURY SUFFICIENT TO SUPPORT STANDING

Unable to genuinely plead that the Attack has led to any actual theft of their identities, Plaintiffs attempt to characterize the Attack *itself* as a "privacy" injury. In essence, Plaintiffs contend that the mere fact that their information was obtained by an unauthorized third party in the Attack is by itself a "privacy" harm—regardless of whether any tangible harm occurred as a result of the exposure of the information. This standing theory also fails.

TransUnion makes clear that intangible harms such as invasions of privacy are only sufficiently "concrete" for Article III standing where they have a "close relationship" to "harms traditionally recognized as providing a basis for lawsuits in American courts." 141 S. Ct. at 2204. To show that a "close relationship" between a claimed intangible harm and a traditionally cognizable harm exists, a plaintiff must show that the necessary components of the analogous and cognizable cause of action exist. *See id.* at 2209. Accordingly, the Supreme Court held that the plaintiffs in *TransUnion* whose inaccurate credit files had never been disseminated could not establish standing by reference to the traditional tort of defamation, because publication (*i.e.*, dissemination) is "essential to liability" in a suit for defamation. *Id.* (quoting Restatement of Torts § 577).

Here, Plaintiffs invoke the tort of "publicity given to private life" as the root of their privacy injury, alleging that the Attack "publicized information relating to the named Plaintiffs, including highly private information such as login IDs, passwords, and phone numbers to cyber criminals, thereby invading their privacy." Am. Compl. ¶ 69. But the facts pled do not bear any "close relationship" to that tort. The tort (also known as "public disclosure of private facts") imposes liability for "publiciz[ing]" "a matter concerning the private life of another," if that matter is "of a kind" that "would be highly offensive to a reasonable person" and "not of

legitimate concern to the public." Restatement (Second) of Torts § 652D (1977).[8] The tort protects the interest "of reputation, with the same overtones of mental distress that are present in libel and slander." William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 398 (1960).[9] Plaintiffs here cannot claim that the minimal information affected in the Attack consists of "facts" about their "private lives," nor can they claim that the information has been widely publicized.

A. Plaintiffs Fail to Adequately Allege the Disclosure of "Private Facts"

For Plaintiffs to invoke an actionable disclosure of "private facts," Plaintiffs must allege a disclosure that reveals "'*intimate details* of plaintiffs' lives.'" *Karimi*, 361 F. Supp. 3d at 980 (emphasis in original) (citation omitted); *see also Chisholm v. Foothill Capital Corp.*, 3 F. Supp. 2d 925, 941 (N.D. Ill. 1998) (recognizing this tort "protect[s] against the disclosure of 'intimate . . . details the publicizing of which would be not merely embarrassing and painful but deeply shocking to the average person subjected to such exposure'" (quoting *Haynes v. Alfred A. Knopf, Inc.*, 8 F.3d 1222, 1234 (7th Cir. 1993))). Qualifying "private matters" include sexual relationships, family quarrels, humiliating illnesses, and intimate personal letters. Restatement (Second) of Torts § 652D cmt. b; *see also, e.g.*, Prosser, *Privacy*, 48 Cal. L. Rev. at 392, 397 (describing tort as consisting of "public disclosure of *embarrassing* private facts about the plaintiff," such as "sexual relations" or "intimate private characteristics or conduct" (emphasis added)); *Gross v. Chapman*, 475 F. Supp. 3d 858, 862 (N.D. Ill. 2020) ("inherently private facts include 'a person's financial, medical, or sexual life, or a peculiarly private fact of an intimate[,] personal nature'" (citation omitted)).

None of the information affected by the Attack is remotely comparable to such "intimate details" or embarrassing "private matters." As an initial matter, Plaintiffs do not even allege that

---

[8] *See also Karimi v. Golden Gate Sch. of L.*, 361 F. Supp. 3d 956, 980 (N.D. Cal. 2019), *aff'd*, 796 F. App'x 462 (9th Cir. 2020) ("The California Supreme Court has 'set forth the elements of the public-disclosure-of-private-facts tort as follows: '(1) public disclosure, (2) of a private fact, (3) which would be offensive and objectionable to the reasonable person, and (4) which is not of legitimate public concern.'" (citation omitted)).

[9] *See Thane Int'l, Inc. v. Hartford Fire Ins. Co.*, No. EDCV061244VAPOPX, 2008 WL 11335049, at *6 (C.D. Cal. Mar. 15, 2008) (explaining that "[t]racing the development of [privacy torts] generally begins with William L. Prosser's influential article classifying the types of interests protected by the law of privacy" (citing Prosser, *Privacy*, 48 Cal. L. Rev. 383)).

the information of theirs that was affected in the Attack could be tied to them personally—while each Plaintiffs' screen name and email was affected by the Attack, Plaintiffs do not allege their screen names and emails even matched their actual identities. Indeed, Rosiak's public filings in this case reveal that his screen name ("roshokk") and his email ("roshokk434@att.net") do *not* match his real name. *Rosiak v. Zynga Inc.*, No. 20-cv-05674-YGR (N.D. Cal. Nov. 9, 2020), *Rosiak* Dkt. 29-1 at 5. It should go without saying that Plaintiffs cannot establish an invasion of their privacy based on the exposure of information that is not even "individually identifiable" to them. *Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017).

But even if the information affected in the Attack were actually traceable to these particular Plaintiffs, it would still not constitute "private facts":

- **Screen names and email addresses (all Plaintiffs).** Email addresses and screen names are public information designed to be shared with others. *See* Ferris Decl. ¶ 7(d) (screen name is how player "would appear to other players"). As this Court has recognized, disclosure of this information thus does not create a cognizable privacy harm. Tr. 23:20-25 ("I don't think emails and screen names gets you there . . . [b]ecause people disclose stuff like that all the time."). Underscoring that email addresses and screen names are not private, Rosiak disclosed both pieces of information in a public filing in this case without seeking any type of sealing order. *Rosiak* Dkt. 29-1 at 5; *see also* Restatement (Second) of Torts § 652D cmt. b (no liability for giving "further publicity to information about the plaintiff that is already public").
- **Phone number and date of birth (Johnson).** Similarly, disclosure of Johnson's phone number and date of birth do not establish a privacy harm with a close relationship to publicity given to private facts. A phone number, like an email address, is designed to be shared to facilitate communication, is often publicly listed, and is plainly not an intimate or embarrassing detail about someone's private life. *See, e.g.*, *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004) ("names, telephone numbers, addresses or social security numbers" furnished by customers

"have [not] been held to be private facts"). And date of birth is a "matter of public record" that the Restatement expressly identifies as insufficient to constitute a "private fact." Restatement (Second) of Torts § 652D cmt. b; *see also Busse*, 813 N.E.2d at 1018 ("Matters of public record—name, address, date of birth and fact of marriage—have been held not to be private facts." (citation omitted)).[10]

- **Passwords (I.C. and Johnson).**[11] Finally, passwords are not "private facts"—*i.e.*, intimate details of a plaintiff's life. *See, e.g.*, *Busse*, 813 N.E.2d at 1018 (social security numbers are not "private information" or "private facts" "as that term is used in the Restatement"). Indeed, a password is not a "fact" at all; it is simply a key to an account. Just as someone who has lost a physical key would not claim that any "fact" about their private life had been "publicized" as a result, Plaintiffs cannot make such a claim about the compromise of an online password. A password is distinct from the information it may be used to obtain. And, as discussed above, Plaintiffs do not allege anyone actually *used* their passwords to obtain access to an account containing intimate or embarrassing details about their lives, much less that anyone then publicized that information. *See supra* at 5-9.

Notwithstanding the nature of the information at issue here, Plaintiffs have previously argued that this case is "on all fours" with *TransUnion*, Surreply at 4, simply because their information "has already been disseminated to cyber criminals." *Id.*; *see also* Tr. 17:18-21 (counsel for Plaintiffs arguing that Plaintiffs have standing under *TransUnion* because "[t]he information is no longer safely on Zynga's servers" but "has been disseminated, or in the words of the Supreme Court in *TransUnion*, it's been published"). But, as the Court recognized, mere

---

[10] Rosiak also claims that his phone number, along with his Facebook name and user ID, were "compromised" from his Facebook account, but, as explained above (at 7-8), he has no basis to connect this information to the Attack. Regardless, as with Johnson, Rosiak cannot claim that his phone number is an intimate fact about his life. Nor can he claim that his Facebook name or user ID constitute private facts either, as both are publicly accessible types of information on Facebook. S*ee* Turner Decl., Ex. C (explaining that a Facebook user's name and user ID are "always public" and "can be seen by anyone").

[11] As discussed above, Zynga's records disprove Rosiak's contention that his password was compromised. *See supra* at 8 n.6, Ferris Decl. ¶ 16.

dissemination of the information at issue here is not sufficient to establish standing. Tr. 32:24-25 (stating that "I do think there's dissemination" but "I don't think that that is necessarily enough"). Indeed, Plaintiffs' argument fundamentally misunderstands *TransUnion*. *TransUnion* did not hold that disclosure of *any* information establishes a cognizable injury; it held that disclosure of credit reports "that labeled the class members as potential terrorists, drug traffickers, or serious criminals" caused a "*reputational* harm associated with the tort of defamation." 141 S. Ct. at 2208-09 (emphasis added). Plaintiffs cannot simply ignore the nature of the information at issue here—which presents neither a reputational harm nor a privacy harm traditionally recognized in American courts.

B. Plaintiffs Fail to Adequately Allege "Publicity"

Plaintiffs also fail to allege facts showing "publicity"—an "essential" element of the tort of publicity given to private facts. *See TransUnion*, 141 S. Ct. at 2209. The meaning of "publicity" in this context is narrow—it requires that the matter be "made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of *public knowledge*." Restatement (Second) of Torts § 652D cmt. a (emphasis added); *see also Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 27 (1994) ("[C]ommon law invasion of privacy by public disclosure of private facts requires that the actionable disclosure be widely published and not confined to a few persons or limited circumstances." (citing Restatement)); *Snipes v. Wilkie*, No. 18-CV-03259-TSH, 2019 WL 1283936, at *7 (N.D. Cal. Mar. 20, 2019) (similar).

The Amended Complaint alleges that "[t]he data breach publicized information relating to the named Plaintiffs, including highly private information such as login IDs, passwords, and phone numbers to cyber criminals," Am. Compl. ¶ 69, and that the phishing and spam emails Plaintiffs have allegedly received are evidence that criminals have "published [Plaintiff's information] on the dark web," *id.* ¶ 114. But the facts alleged do not amount to publicity—information posted to the dark web or "published" to cyber criminals is not communicated to "the public at large" and is unlikely to become "public knowledge." Restatement (Second) of Torts § 652D cmt. a; *see also, e.g.*, *Warfield v. Peninsula Golf & Country Club*, 214 Cal. App.

3d 646, 660 (1989) (holding that "the required threshold allegation of a general public disclosure [was] absent" where disclosure occurred in country club's membership newsletter). Harm to *reputation* is the core injury associated with this tort, and thus the disclosure must be so public as to implicate that concern. *See* Prosser, *Privacy*, 48 Calif. L. Rev. at 398.

The "publicity" requirement also provides an additional point of distinction between this case and *TransUnion.* Plaintiffs have previously suggested that *any* disclosure or dissemination rises to the level of publicity sufficient to state a privacy harm. *See, e.g.*, Tr. 17:18-21 (counsel for Plaintiffs arguing that "[t]he information is no longer safely on Zynga's servers" but "has been disseminated, or in the words of the Supreme Court in *TransUnion*, it's been published"); Surreply at 4 (arguing that "private information has already been disseminated to cyber criminals as a result of Zynga's inadequate security protocols"). But in *TransUnion*, the Court discussed the "*publication*" requirement for defamation. 141 S. Ct. at 2209 (citing Restatement of Torts § 577 cmt. a). That requirement differs sharply from "publicity" under public disclosure of private facts, because "publication" for defamation purposes "includes any communication by the defendant to a third party," whereas "publicity" for Plaintiffs' purposes here means the matter is "communicat[ed] . . . to the public at large." Restatement (Second) of Torts § 652D cmt. a (explaining that "publicity" as used in § 652D "differs from 'publication,' as that term is used in § 577 in connection with liability for defamation"); *see also, e.g.*, *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1062 (N.D. Cal. 2014) (recognizing same distinction and dismissing public disclosure of private facts claim for failure to allege publicity). Thus, while dissemination to even one third party sufficed in *TransUnion*, 141 S. Ct. at 2212-13, Plaintiffs must allege far broader dissemination to demonstrate a cognizable harm based on a theory of publicity given to private information. They fail to do so. [12]

[12] Notably, Plaintiffs' alleged privacy harms also turn exclusively on the actions of *third parties*—specifically, criminal hackers and downstream identity thieves. None of their allegations allege any intentional publication or intrusion *by Zynga*. That not only dooms their privacy claims on the merits, *see, e.g.*, *Armijo v. Yakima HMA, LLC*, No. 11-CV-3114-TOR, 2012 WL 2576624, at *2 (E.D. Wash. July 3, 2012) (citing Restatement and explaining that public disclosure of private facts requires that "the defendant [ ] intentionally disclosed private facts"), but also weighs against standing, because they have failed to establish the elements

VI. PLAINTIFFS LACK STANDING FOR INJUNCTIVE RELIEF

Finally, Plaintiffs lack standing to seek injunctive relief because they cannot show a "real and immediate threat of repeated injury." *O'Shea v. Littleton*, 414 U.S. 488, 496 (1974). Indeed, given the nature of the information affected and the passage of nearly two years with no concrete, adverse effects, Plaintiffs cannot show any imminent risk of future harm from *this* data breach. *See supra* at 11. That failure forecloses any possibility that they could show a "sufficiently imminent and substantial" risk of harm from a *future* breach of their accounts. *TransUnion*, 141 S. Ct. at 2210. And any possible risk from a future data breach is especially speculative because Zynga reset all passwords affected by the Attack, Ferris Decl. ¶ 18, and Plaintiffs allege they stopped playing Zynga games either well before the Attack, *see* Am. Compl. ¶¶ 17, 29, 32, or upon learning of the Attack, *id.* ¶ 8. There is thus no basis to infer that they have ever created new passwords that are currently stored by Zynga. Accordingly, Plaintiffs cannot show the immediate threat of repeated injury necessary to obtain prospective relief.

VII. CONCLUSION

For all of the foregoing reasons, the Court should grant Zynga's Motion to Dismiss, and dismiss Plaintiffs' Amended Complaint without leave to amend.

DATED: September 20, 2021

LATHAM & WATKINS LLP

/s/ Elizabeth L. Deeley

Elizabeth L. Deeley (CA Bar No. 230798)
elizabeth.deeley@lw.com
505 Montgomery Street, Suite 2000
San Francisco, California 94111-6538
Telephone: +1.415.391.0600
Facsimile: +1.415.395.8095

Susan E. Engel (*pro hac vice*)
susan.engel@lw.com
555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Telephone: +1.202.637.2200
Facsimile: +1.202.637.2201

"essential to liability" for the privacy torts upon which they rely. *TransUnion*, 141 S. Ct. at 2209.

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
1271 Avenue of the Americas
New York, NY 10020
Telephone: +1.212.906.1200
Facsimile: +1.212.751.4864

Attorneys for Defendant *Zynga Inc.*